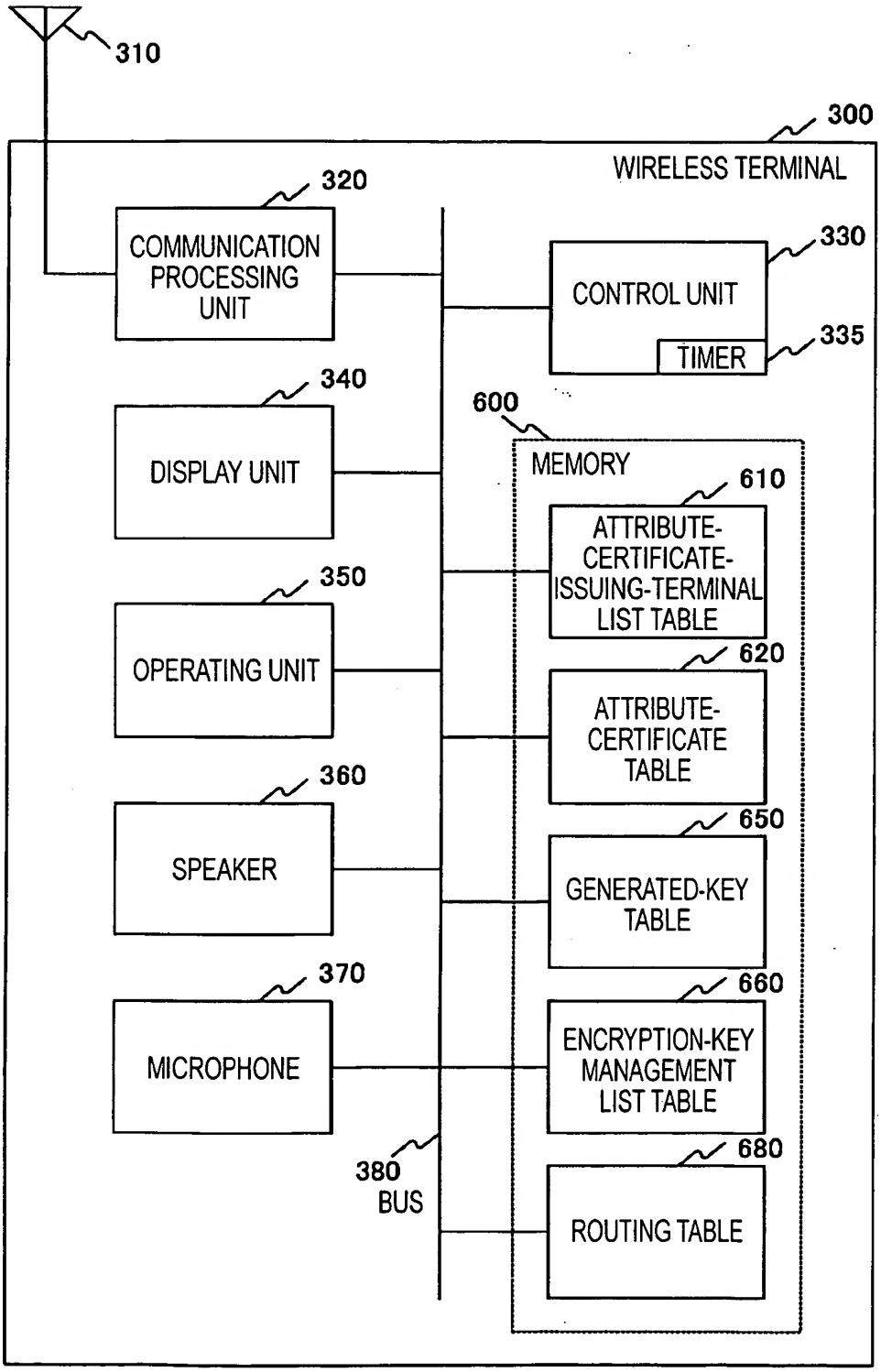

310
300
WIRELESS TERMINAL
320
COMMUNICATION PROCESSING UNIT
330
CONTROL UNIT
335
TIMER
340
DISPLAY UNIT
600
MEMORY
610
ATTRIBUTE-CERTIFICATE-ISSUING-TERMINAL LIST TABLE
350
OPERATING UNIT
620
ATTRIBUTE-CERTIFICATE TABLE
360
SPEAKER
650
GENERATED-KEY TABLE
370
MICROPHONE
660
ENCRYPTION-KEY MANAGEMENT LIST TABLE
380
BUS
680
ROUTING TABLE

FIG. 1

610

611 TERMINAL IDENTIFIER	612 PUBLIC KEY CERTIFICATE
TERMINAL X	PUBLIC KEY CERTIFICATE X
TERMINAL Y	PUBLIC KEY CERTIFICATE Y
⋮	⋮

FIG. 2

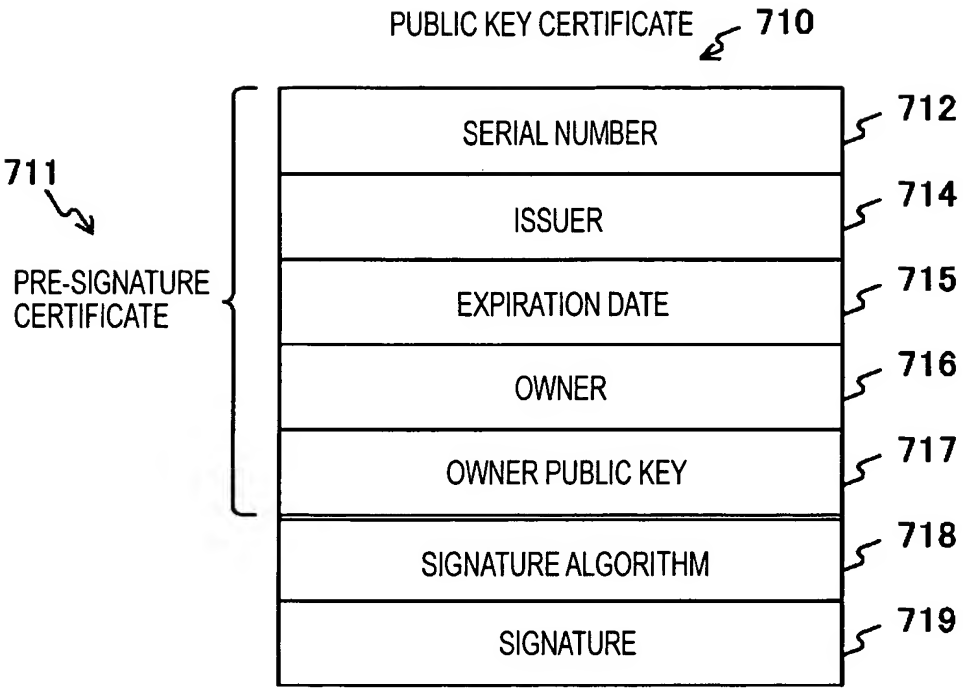

PUBLIC KEY CERTIFICATE
710
711
PRE-SIGNATURE CERTIFICATE
SERIAL NUMBER
712
ISSUER
714
EXPIRATION DATE
715
OWNER
716
OWNER PUBLIC KEY
717
SIGNATURE ALGORITHM
718
SIGNATURE
719

FIG. 3

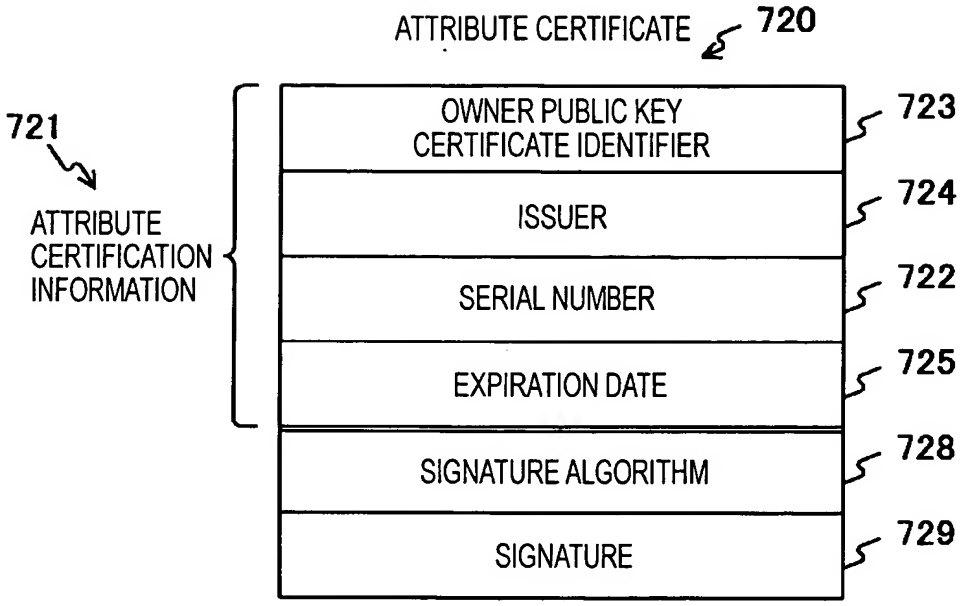

ATTRIBUTE CERTIFICATE
720
721
ATTRIBUTE CERTIFICATION INFORMATION
OWNER PUBLIC KEY CERTIFICATE IDENTIFIER
723
ISSUER
724
SERIAL NUMBER
722
EXPIRATION DATE
725
SIGNATURE ALGORITHM
728
SIGNATURE
729

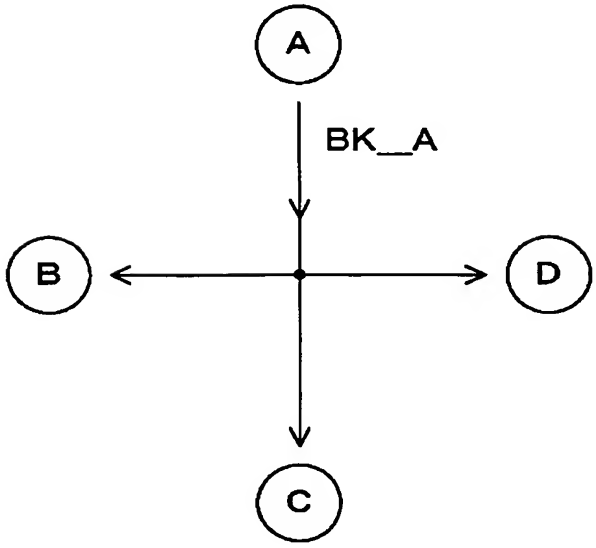
FIG. 4

660

661 TERMINAL IDENTIFIER	662 UNICAST ENCRYPTION KEY	663 BROADCAST ENCRYPTION KEY
TERMINAL B	UK__AB	BK__B
TERMINAL C	UK__AC	BK__C
TERMINAL D	UK__AD	BK__D
⋮	⋮	⋮

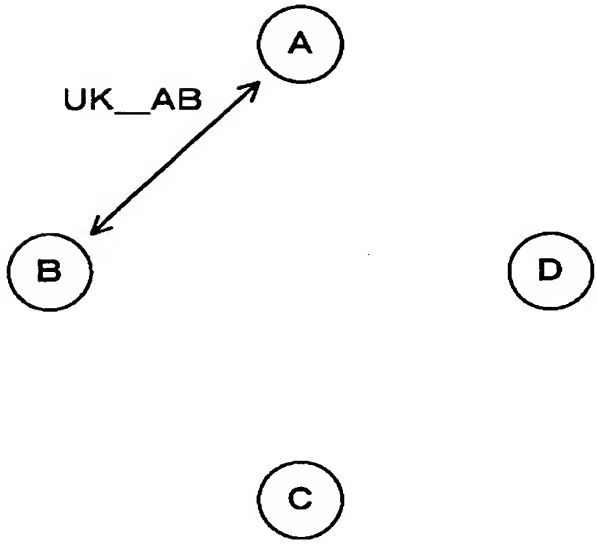
FIG. 5

FIG. 6A



BROADCAST KEY

FIG. 6B



UNICAST KEY

680

681 END-TERMINAL IDENTIFIER	682 FORWARDING-TERMINAL IDENTIFIER	683 EXPIRATION TIME
TERMINAL B	TERMINAL B	1:30
TERMINAL C	TERMINAL C	0:50
TERMINAL D	TERMINAL D	0:30
⋮	⋮	⋮

FIG. 7

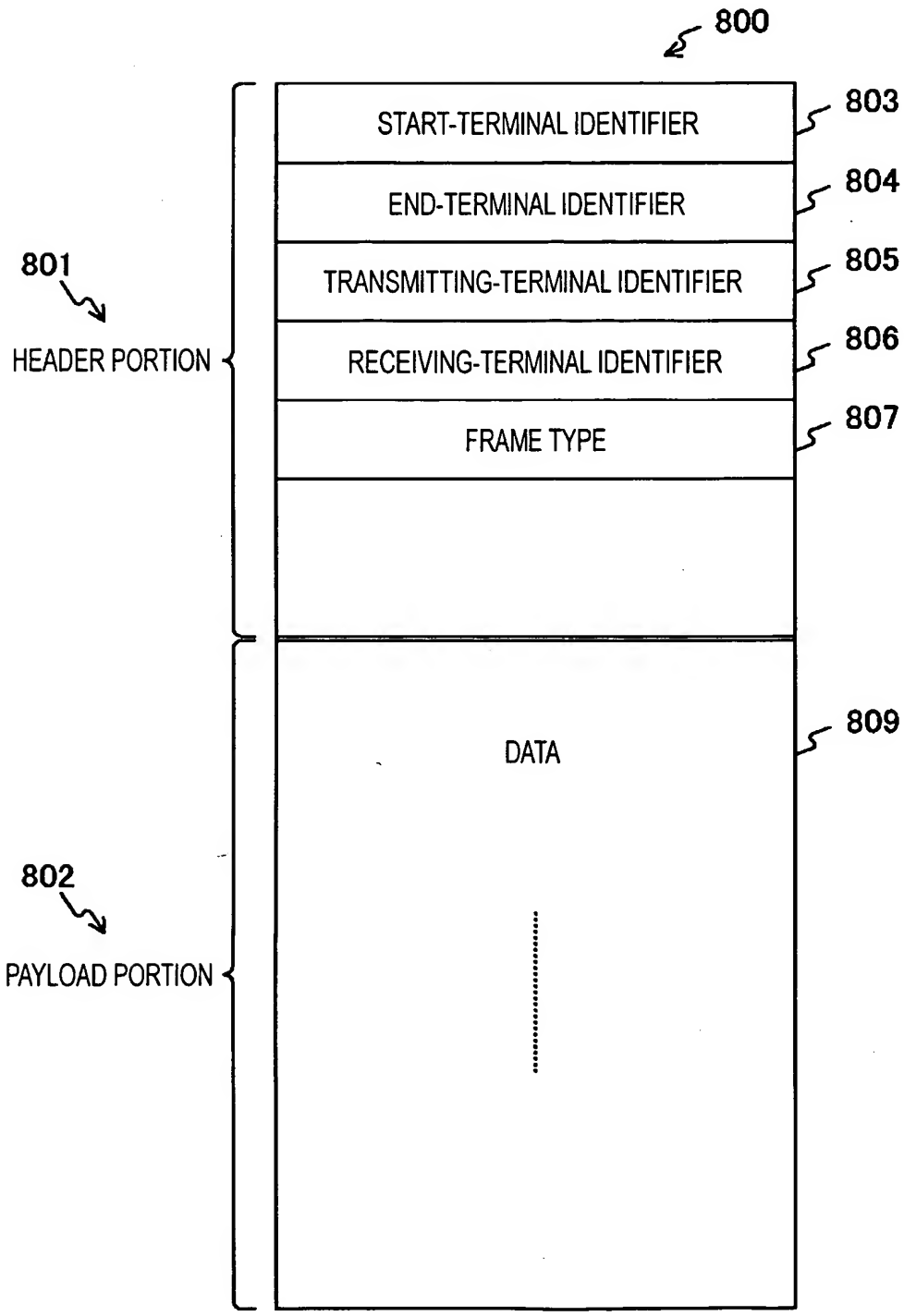

800
START-TERMINAL IDENTIFIER
803
END-TERMINAL IDENTIFIER
804
801
TRANSMITTING-TERMINAL IDENTIFIER
805
HEADER PORTION
RECEIVING-TERMINAL IDENTIFIER
806
FRAME TYPE
807
DATA
809
802
PAYLOAD PORTION

FIG. 8

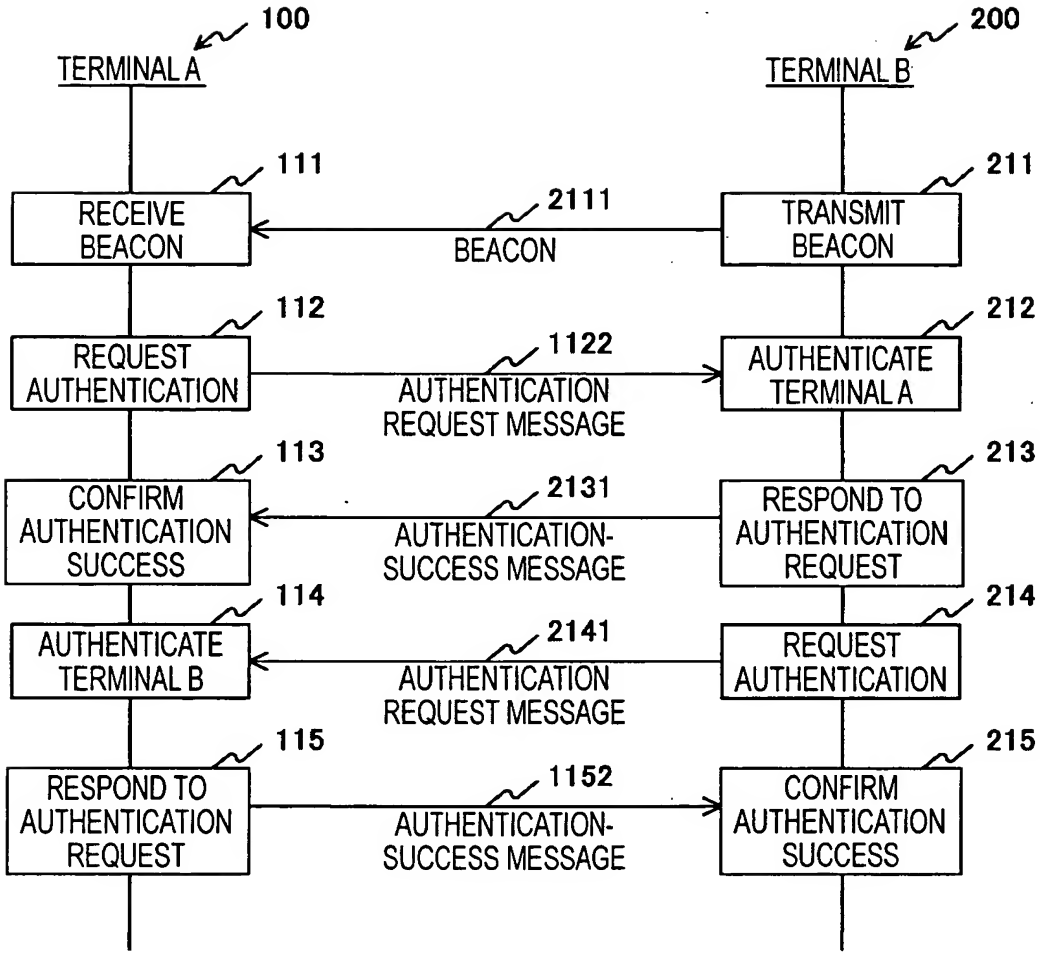

100
TERMINAL A
200
TERMINAL B
111
RECEIVE BEACON
2111
BEACON
211
TRANSMIT BEACON
112
REQUEST AUTHENTICATION
1122
AUTHENTICATION REQUEST MESSAGE
212
AUTHENTICATE TERMINAL A
113
CONFIRM AUTHENTICATION SUCCESS
2131
AUTHENTICATION-SUCCESS MESSAGE
213
RESPOND TO AUTHENTICATION REQUEST
114
AUTHENTICATE TERMINAL B
2141
AUTHENTICATION REQUEST MESSAGE
214
REQUEST AUTHENTICATION
115
RESPOND TO AUTHENTICATION REQUEST
1152
AUTHENTICATION-SUCCESS MESSAGE
215
CONFIRM AUTHENTICATION SUCCESS

FIG. 9

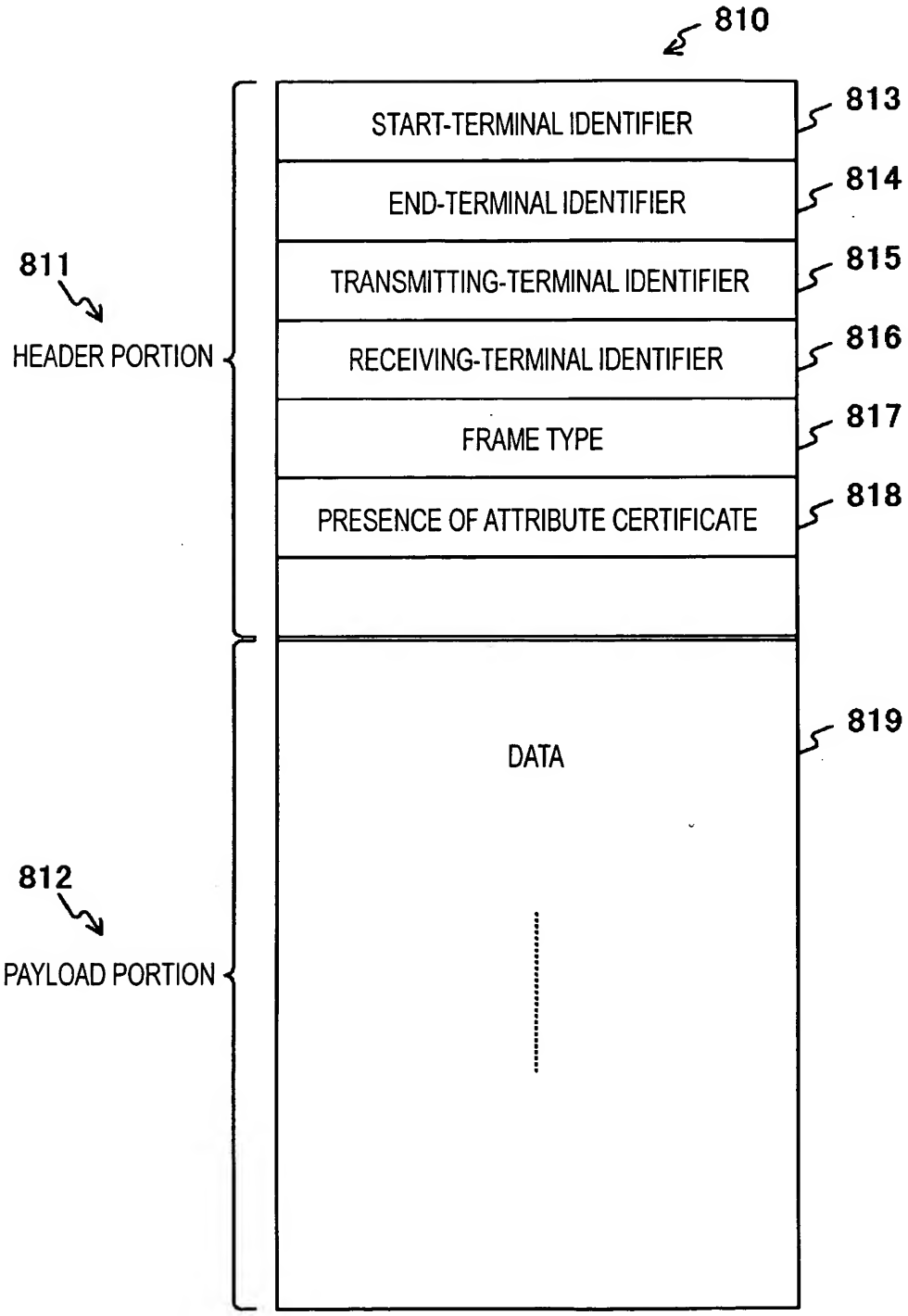

810
START-TERMINAL IDENTIFIER
813
END-TERMINAL IDENTIFIER
814
TRANSMITTING-TERMINAL IDENTIFIER
815
RECEIVING-TERMINAL IDENTIFIER
816
FRAME TYPE
817
PRESENCE OF ATTRIBUTE CERTIFICATE
818
DATA
819
811
HEADER PORTION
812
PAYLOAD PORTION

FIG. 10

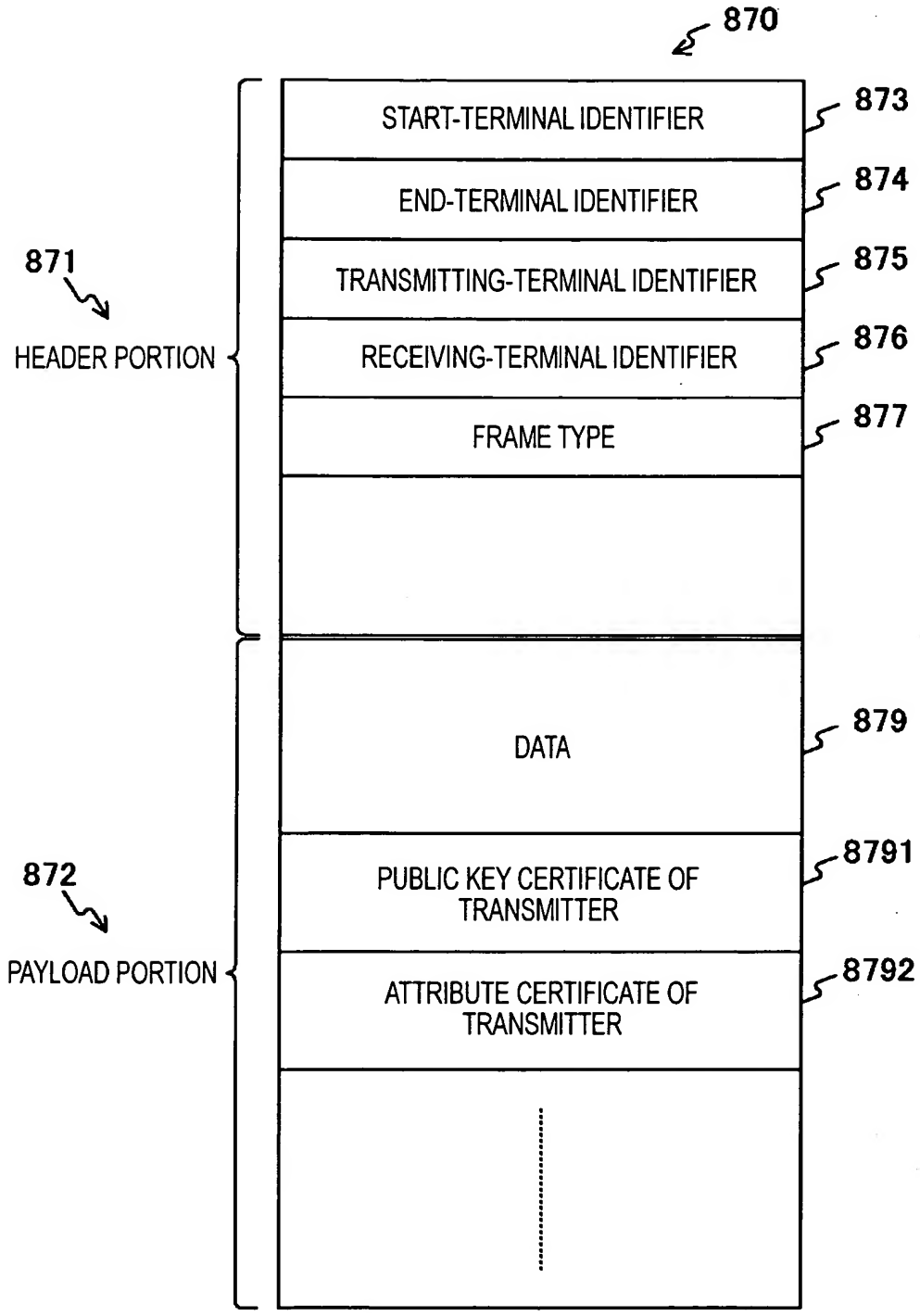

870
START-TERMINAL IDENTIFIER
873
END-TERMINAL IDENTIFIER
874
871
TRANSMITTING-TERMINAL IDENTIFIER
875
HEADER PORTION
RECEIVING-TERMINAL IDENTIFIER
876
FRAME TYPE
877
DATA
879
872
PUBLIC KEY CERTIFICATE OF TRANSMITTER
8791
PAYLOAD PORTION
ATTRIBUTE CERTIFICATE OF TRANSMITTER
8792

FIG. 11

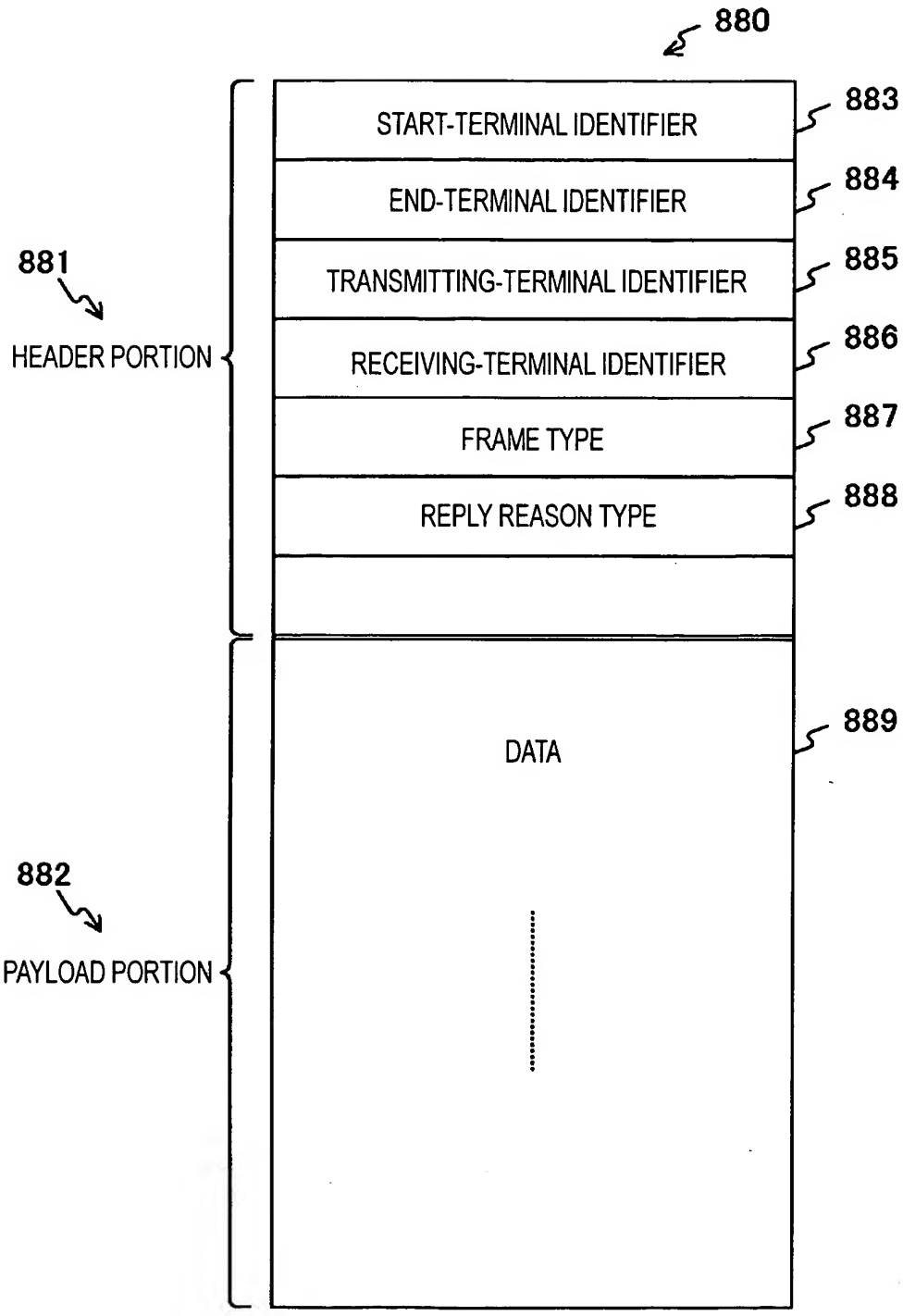

880
START-TERMINAL IDENTIFIER
883
END-TERMINAL IDENTIFIER
884
881
TRANSMITTING-TERMINAL IDENTIFIER
885
HEADER PORTION
RECEIVING-TERMINAL IDENTIFIER
886
FRAME TYPE
887
REPLY REASON TYPE
888
DATA
889
882
PAYLOAD PORTION

FIG. 12

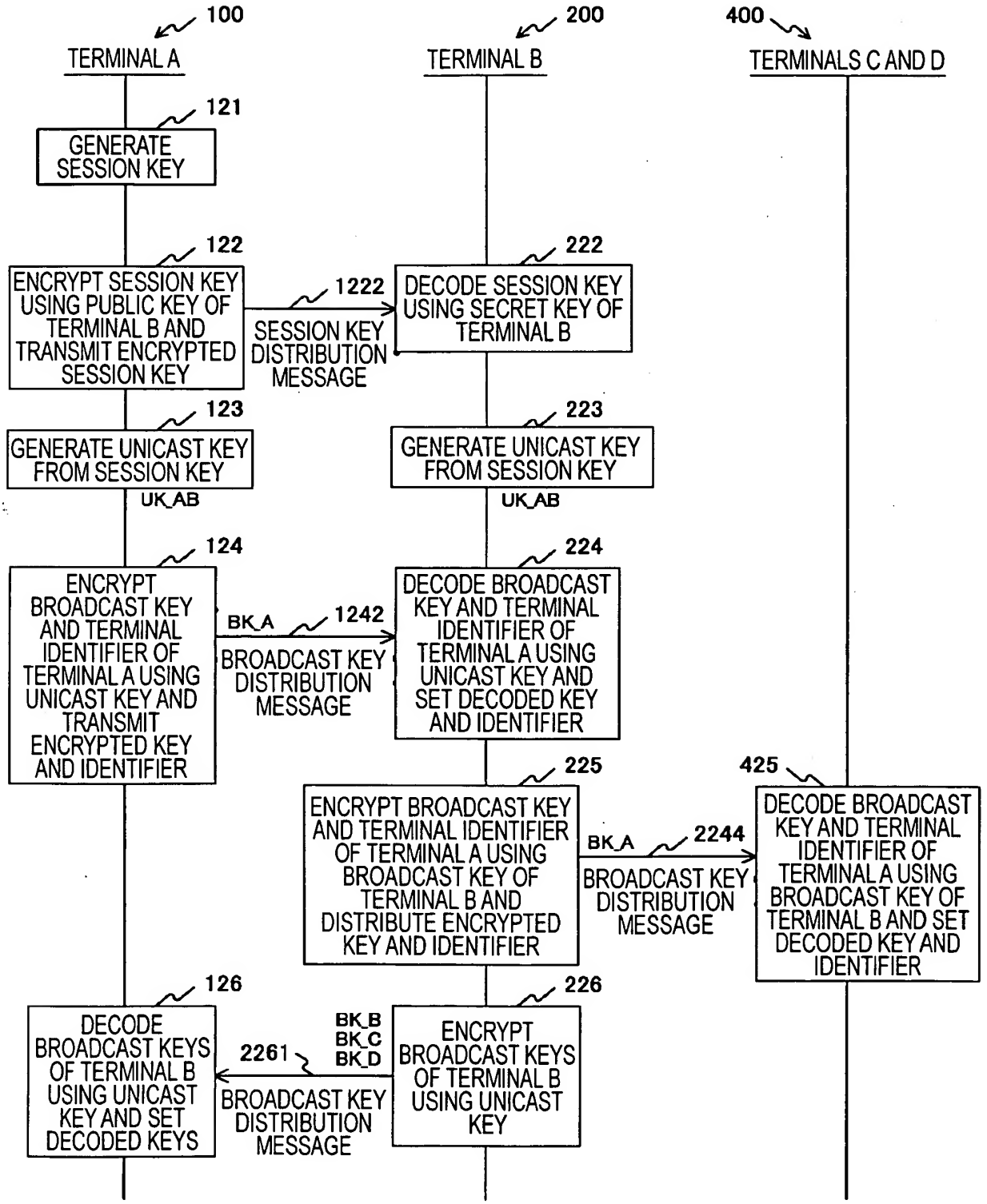

100
TERMINAL A
200
TERMINAL B
400
TERMINALS C AND D
121
GENERATE SESSION KEY
122
ENCRYPT SESSION KEY USING PUBLIC KEY OF TERMINAL B AND TRANSMIT ENCRYPTED SESSION KEY
1222
SESSION KEY DISTRIBUTION MESSAGE
222
DECODE SESSION KEY USING SECRET KEY OF TERMINAL B
123
GENERATE UNICAST KEY FROM SESSION KEY
223
GENERATE UNICAST KEY FROM SESSION KEY
UK_AB
UK_AB
124
ENCRYPT BROADCAST KEY AND TERMINAL IDENTIFIER OF TERMINAL A USING UNICAST KEY AND TRANSMIT ENCRYPTED KEY AND IDENTIFIER
BK_A
1242
BROADCAST KEY DISTRIBUTION MESSAGE
224
DECODE BROADCAST KEY AND TERMINAL IDENTIFIER OF TERMINAL A USING UNICAST KEY AND SET DECODED KEY AND IDENTIFIER
225
ENCRYPT BROADCAST KEY AND TERMINAL IDENTIFIER OF TERMINAL A USING BROADCAST KEY OF TERMINAL B AND DISTRIBUTE ENCRYPTED KEY AND IDENTIFIER
425
BK_A
2244
BROADCAST KEY DISTRIBUTION MESSAGE
DECODE BROADCAST KEY AND TERMINAL IDENTIFIER OF TERMINAL A USING BROADCAST KEY OF TERMINAL B AND SET DECODED KEY AND IDENTIFIER
126
DECODE BROADCAST KEYS OF TERMINAL B USING UNICAST KEY AND SET DECODED KEYS
BK_B
BK_C
BK_D
2261
BROADCAST KEY DISTRIBUTION MESSAGE
226
ENCRYPT BROADCAST KEYS OF TERMINAL B USING UNICAST KEY

FIG. 13

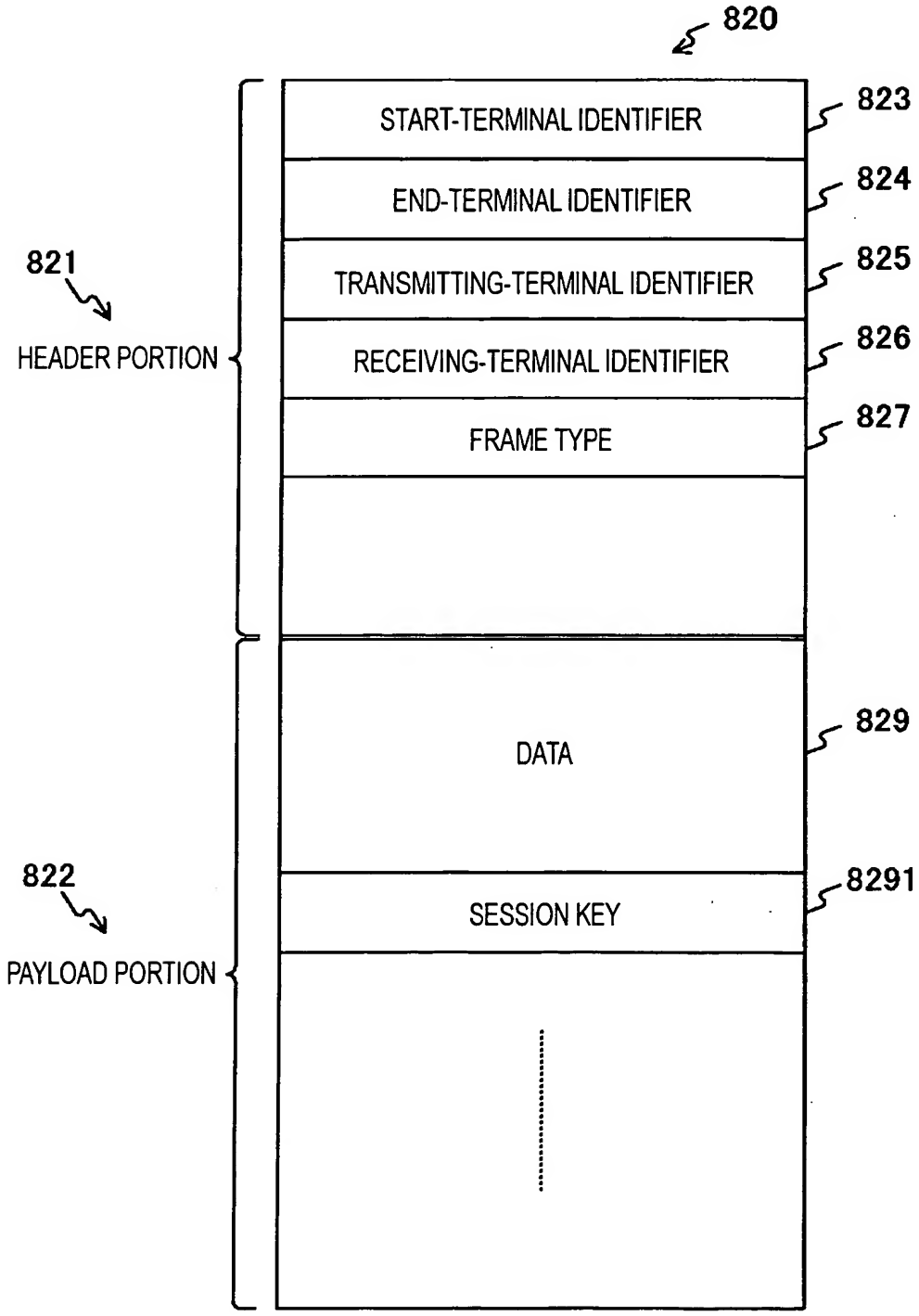

820
START-TERMINAL IDENTIFIER
823
END-TERMINAL IDENTIFIER
824
821
TRANSMITTING-TERMINAL IDENTIFIER
825
HEADER PORTION
RECEIVING-TERMINAL IDENTIFIER
826
FRAME TYPE
827
DATA
829
822
SESSION KEY
8291
PAYLOAD PORTION

FIG. 14

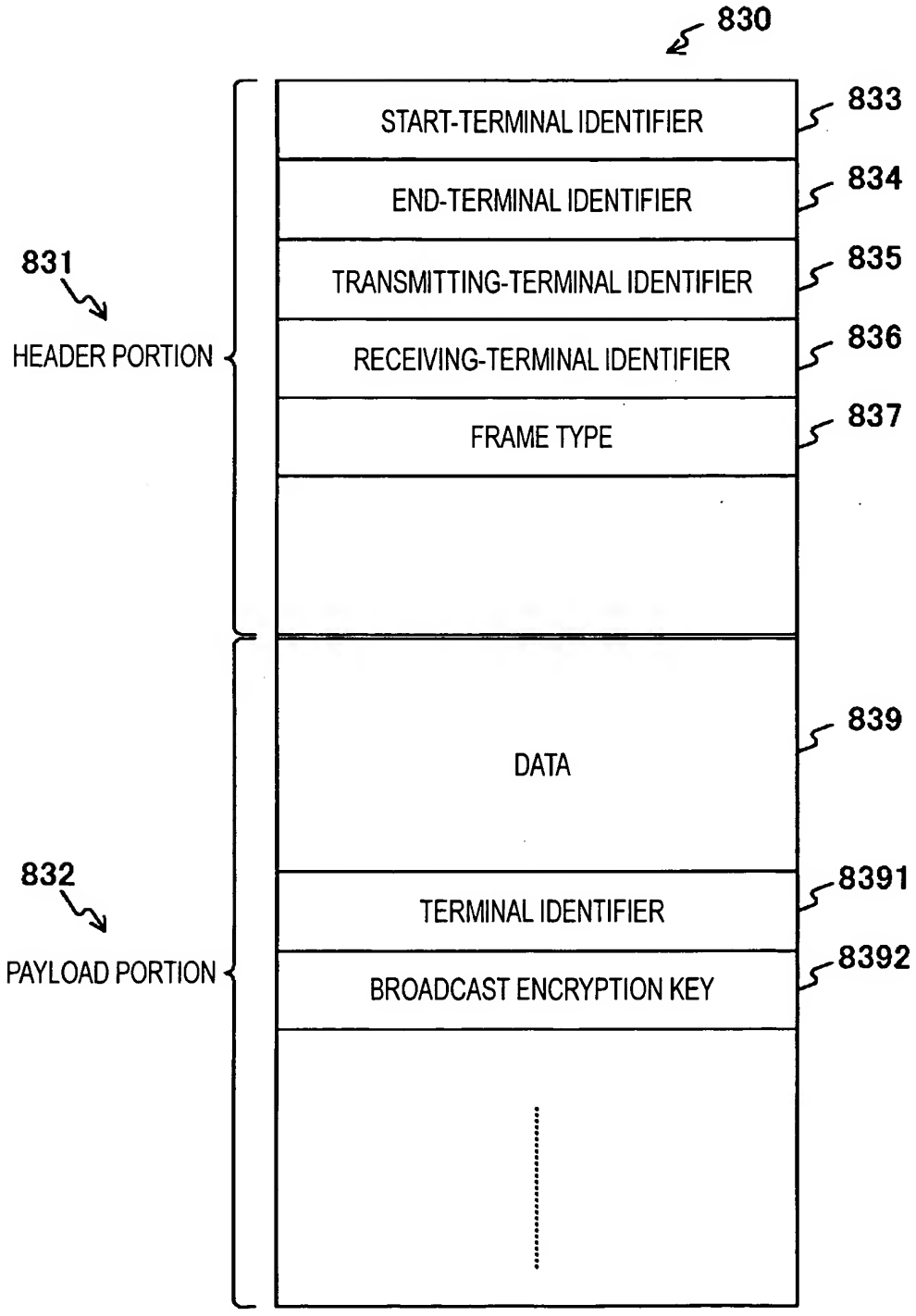

830
START-TERMINAL IDENTIFIER
833
END-TERMINAL IDENTIFIER
834
831
TRANSMITTING-TERMINAL IDENTIFIER
835
HEADER PORTION
RECEIVING-TERMINAL IDENTIFIER
836
FRAME TYPE
837
DATA
839
832
TERMINAL IDENTIFIER
8391
PAYLOAD PORTION
BROADCAST ENCRYPTION KEY
8392

FIG. 15

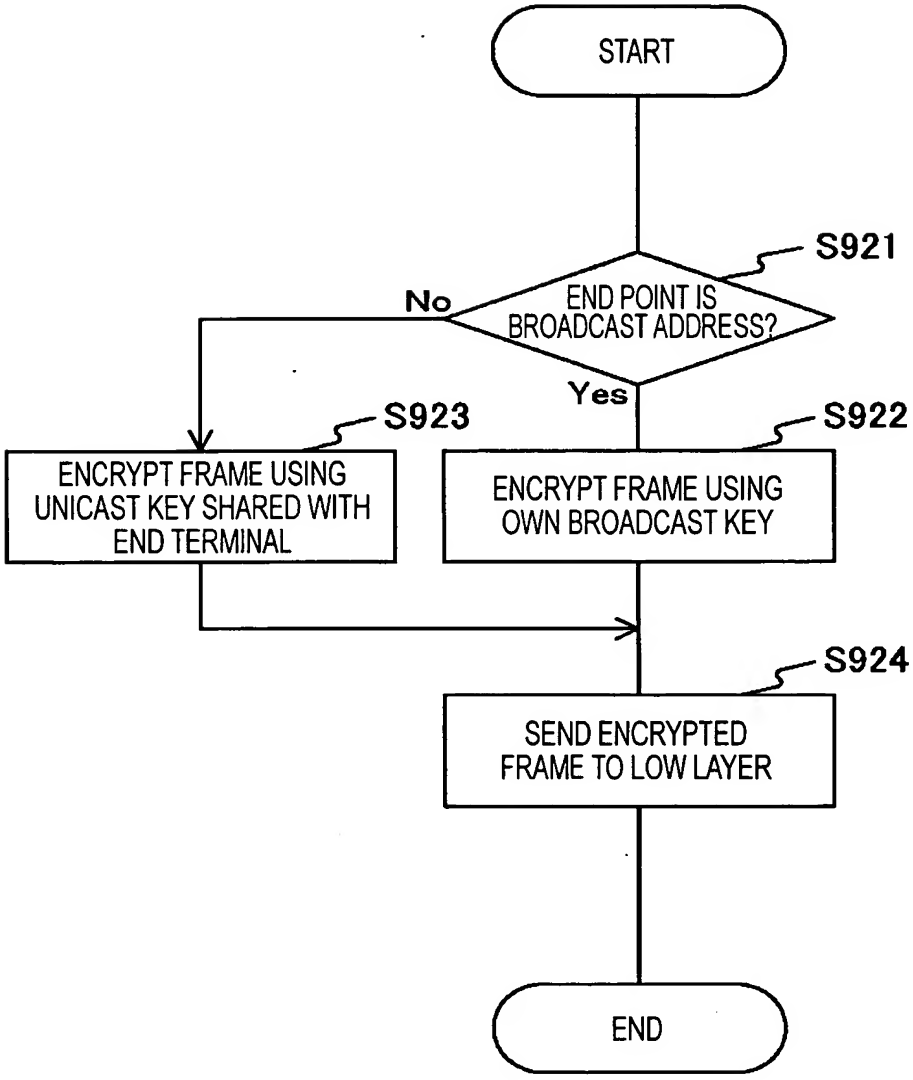

START
S921
END POINT IS BROADCAST ADDRESS?
No
Yes
S923
ENCRYPT FRAME USING UNICAST KEY SHARED WITH END TERMINAL
S922
ENCRYPT FRAME USING OWN BROADCAST KEY
S924
SEND ENCRYPTED FRAME TO LOW LAYER
END

FIG. 16

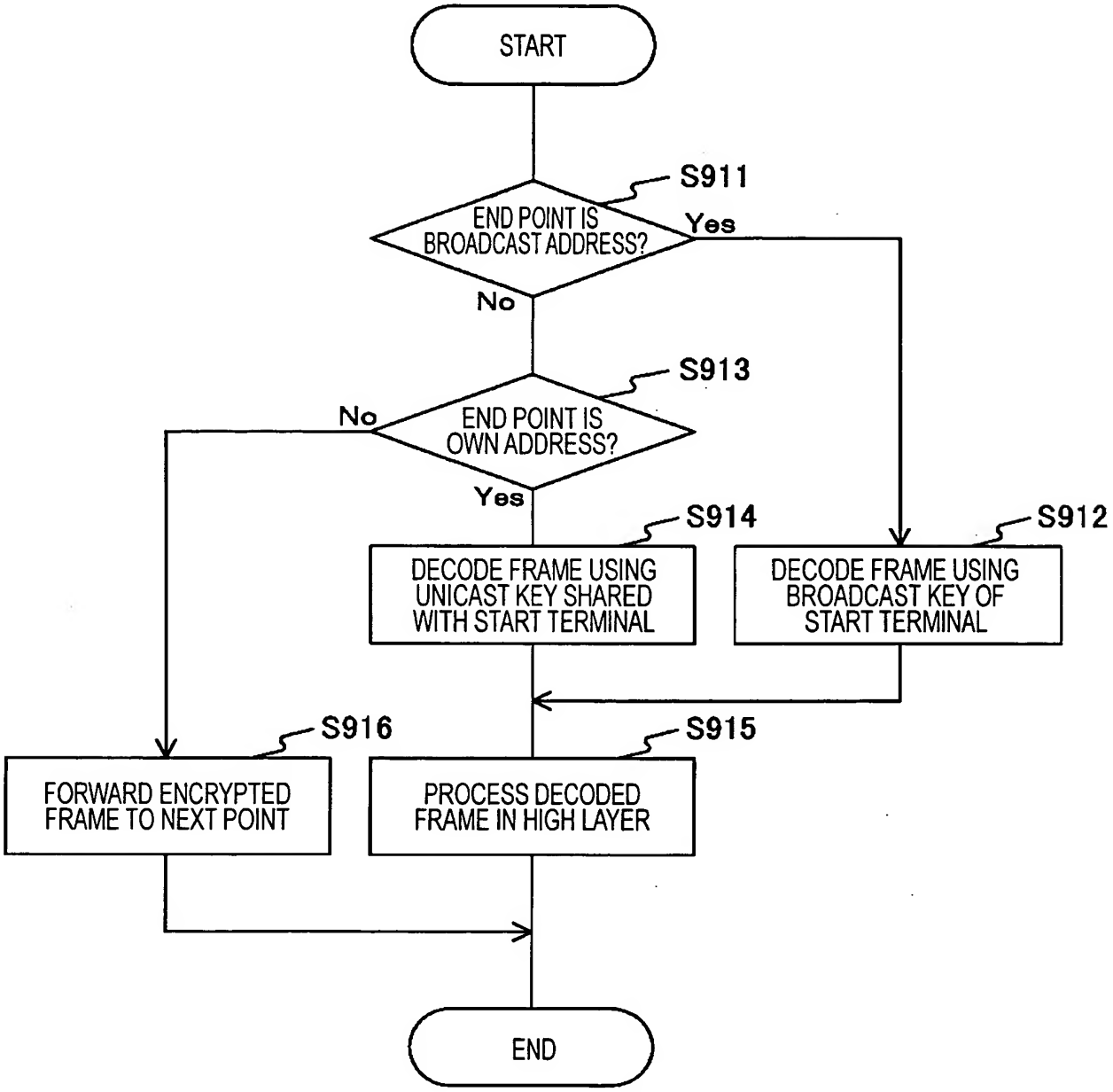

START
S911
END POINT IS BROADCAST ADDRESS?
Yes
No
S913
No
END POINT IS OWN ADDRESS?
Yes
S914
S912
DECODE FRAME USING UNICAST KEY SHARED WITH START TERMINAL
DECODE FRAME USING BROADCAST KEY OF START TERMINAL
S916
S915
FORWARD ENCRYPTED FRAME TO NEXT POINT
PROCESS DECODED FRAME IN HIGH LAYER
END

FIG. 17